2021-07-24

Information Security Risk Assessment

Kuzminykh, I

10.3390/encyclopedia1030050
Encyclopedia
MDPI

encyclopedia

MDPI

Entry

Information Security Risk Assessment

Ievgeniia Kuzminykh [1,*], Bogdan Ghita [2], Volodymyr Sokolov [3] and Taimur Bakhshi [4]

1 Department of Informatics, King's College London, London WC2R 2ND, UK
2 School of Engineering, Computing and Mathematics, University of Plymouth, Plymouth PL4 8AA, UK; bogdan.ghita@plymouth.ac.uk
3 Department of Information and Cyber Security, Borys Grinchenko Kyiv University, 04212 Kyiv, Ukraine; v.sokolov@kubg.edu.ua
4 Center for Information Management and Cyber Security, Foundation for Advancement of Science & Technology, Lahore 54770, Pakistan; taimur.bakhshi@nu.edu.pk
* Correspondence: ievgeniia.kuzminykh@kcl.ac.uk

Definition: Information security risk assessment is an important part of enterprises' management practices that helps to identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. Risk management refers to a process that consists of identification, management, and elimination or reduction of the likelihood of events that can negatively affect the resources of the information system to reduce security risks that potentially have the ability to affect the information system, subject to an acceptable cost of protection means that contain a risk analysis, analysis of the "cost-effectiveness" parameter, and selection, construction, and testing of the security subsystem, as well as the study of all aspects of security.

Keywords: information risk management; security risk assessment; risk classification; OCTAVE; CRAMM; RiskWatch; fuzzy logic

Citation: Kuzminykh, I.; Ghita, B.; Sokolov, V.; Bakhshi, T. Information Security Risk Assessment. *Encyclopedia* **2021**, *1*, 602–617. https://doi.org/10.3390/encyclopedia1030050

Academic Editor: Sangheon Pack

Received: 27 April 2021
Accepted: 19 July 2021
Published: 24 July 2021

1. Introduction

Over time, the complexity of information systems is increasing, and, therefore, the issues of information security are becoming increasingly important for any organization. In this context, particular attention is paid to the analysis and assessment of information security risks as a necessary component of an integrated approach to information security.

Typical analysis (and the associated assessment) of information security risks is performed during the information security audit of a system or the design stage. The main task of an information security audit is to assess the ability and effectiveness of control mechanisms applied to the information technology components, as well as the architecture of information systems in general. An information security audit includes many tasks, such as assessing the effectiveness of the information processing system, assessing the security of the technologies used, the processing process, and management of the automated system. The overall purpose of an information security audit is to ensure the confidentiality, integrity, and availability of an organization's assets. Information security risk assessment is also an integral part of an information security audit.

Depending on the result of their evaluation, methodologies for assessing information security risks can be either quantitative or qualitative. The output of the algorithm of a quantitative methodology is the numerical value of risk. The input data for evaluation are usually used to collect information about adverse or unexpected events in the information security system, which may jeopardize the protection of information (information security incidents). However, the frequent lack of sufficient statistics leads to a decrease in the accuracy and relevance of the results.

Qualitative techniques are more common, as they use overly simplistic scales, which usually contain three levels of risk assessment (low, medium, high). The assessment is carried out by interviewing experts, and intelligent methods are still insufficiently used.

It is apparent that both of the above options have a number of inherent shortcomings. In order to overcome them, recent research focused on identifying alternative techniques that would be both more accurate and more adaptive, as the constant emergence of new sources of threats often renders existing methodologies inaccurate and ineffective. Among the promising methods, there are models based on solving uncertainty problems such as fuzzy logic models and artificial neural networks.

Existing textbooks and studies provide a substantial amount of information, describing either the theoretical concept, a novel approach, or a specific case study implementation. While relevant for specific audiences, such studies are either too extensive or too specific, hence not providing a summary for potential researchers and adopters in the area of information security risk assessment. This entry provides an analysis and comparison of existing methods of information security risk assessment, highlighting their common features, benefits, and shortcomings. The structure of the entry follows closely the concept of information security risk. Section 2 provides a definition, followed in Section 3 by a comparative review of the two main categories of risk analysis (qualitative and quantitative). After the necessary theoretical context is provided, Section 4 provides an extensive analysis of proposed information security risk assessment approaches, including CRAMM, FRAP, OCTAVE, and RiskWatch. Section 5 reviews the limitations shared by the existing techniques and provides possible solutions to overcome them, and then Section 6 concludes the entry.

2. Concept of Information Security Risk

Risk, in a wider sense, is the probability of an event that entails certain losses (for example, physical injury, loss of property, damage to the organization, etc.). Information security risk is the potential probability of using vulnerabilities of an asset or group of assets as a specific threat to damage the organization [1].

The main features of risk are inconsistency, alternativeness, and uncertainty [2]. Classification of information risks is shown in Figure 1 and classified into five groups [3,4].

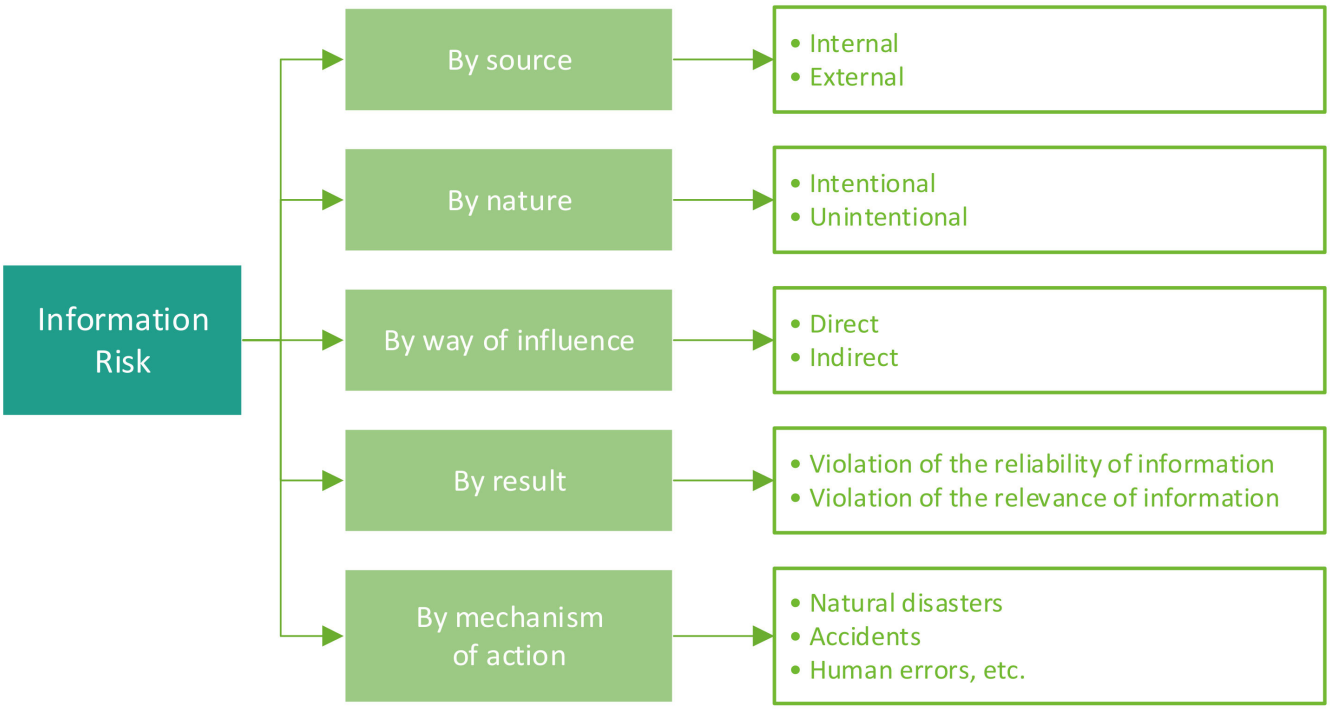

Figure 1. Classification of information risks.

Three additional terms are necessary to describe the risk assessment spectrum boundaries. An inconsistency in risk emerges when the subjective assessment does not adequately and reliably assess and describe the objectively existing risky actions. An alternativeness is the need to choose from two or more possible solutions or actions. If there is no choice, then there are no risky situations and, consequently, risk. Uncertainty is the incompleteness or inaccuracy of information about the conditions of the decision [5]. The existence of risk in itself is possible only when decisions are taken in absence of or with insufficient information about the implications of a decision. These features can lead to serious difficulties in the risk assessment process.

Risk analysis includes a process of risk assessment and potential methods to reduce risks or reduce the associated adverse effects [6]. The concept of risk analysis did not originate with information-related assets, as it generically focuses on two main characteristics: probability and impact of an event onto an organization. In the context of information security, the impact represents the likely damage caused to an organization as a result of information security breaches, taking into account the possible consequences of loss of confidentiality, integrity, or availability of information or other assets. The probability estimates the likelihood of such a breach, taking into account existing threats and vulnerabilities, as well as implemented information security management measures. The level of damage is a monetary parameter and an equivalent of the cost, and the cost can be calculated according to the methodology proposed in [7].

In order to evaluate the level of threat and potential impact of an event, an analysis is carried out, using various tools and methods, on the existing information security processes. Based on the results of this analysis, the highest risks are highlighted, which should be perceived as dangerous threats, requiring immediate additional protective measures.

3. Qualitative and Quantitative Approaches for Risk Analysis

Information security risk analysis can be divided into two types: qualitative and quantitative. Qualitative analysis identifies factors, areas, and types of risks and it typically uses human interaction, for instance, through workshops or interviews, to generate its inputs. Following data collection, risk manager analysis is applied in a qualitative rather than quantitative way. While the process may not satisfy a numerical model, it is often employed for its ability to translate the complexity surrounding the risks studied and to draw relationships between apparently inconsequential pieces of information.

Different types of qualitative analysis can be conducted, for instance, looking at transcripts of the interviews conducted or of the topics discussed during workshops and using some kind of thematic analysis. This can, for instance, be based on analyzing the discourse used, as language can enlighten details about the environment and context of risks.

Different types of qualitative analysis can be conducted. A time-consuming but convenient approach is to apply a thematic analysis to the transcripts of the interviews conducted or the topics discussed during workshops. This can, for instance, be based on analyzing the discourse used, as human language can highlight specific details about the environment and context of risks. Given its input, qualitative risk assessment represents an effective way to consider interrelationships in business areas and hence to be able to assess not only the technical aspects but also the issues arising from *people* and *processes*.

For qualitative risk assessment, the main focus is on the *likelihood* of an event rather than its statistical probability. These likelihoods are derived from analyzing the threats and vulnerabilities, and then generating a qualitative or quantitative value for the asset or assets that may be affected (impact):

$$Risk = Threat \times Vulnerability \times Impact \quad (1)$$

where $Threat \times Vulnerability$ is likelihood.

One example of qualitative risk rating methodology is the OWASP (Open Web Application Security Project) Risk Rating Methodology [8]. Following its analysis, OWASP

generates a summary similar to the one presented by Figure 2a, where Impact and Likelihood are qualitatively evaluated as Low, Medium, or High. Another methodology is the SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis, also known as the SWOT matrix, a tool that is intended to identify and assess the internal factors (strengths and weaknesses) and also external factors including opportunities and threats of a product, project, or a business. SWOT produces a 2 × 2 matrix similar to the one presented by Figure 2b. As visible in the matrix, the focus of the analysis is the external/internal location of the identified characteristics and their negative/positive impact on the organization. Given the combination of the two variables, the respective characteristic is qualified as a strength, weakness, opportunity, or threat and appropriately added to the respective field. Following the analysis, the matrix is fully populated with attributes; typical examples of this methodology can be found in [9,10].

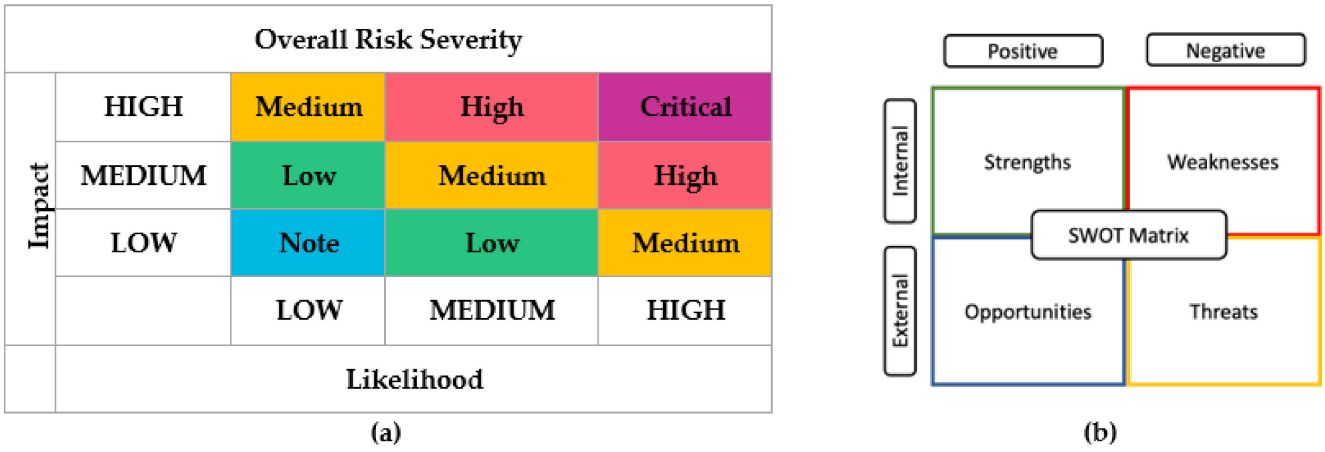

Figure 2. Risk estimation matrix: (**a**) OWASP Risk Rating Methodology; (**b**) SWOT matrix.

In contrast, quantitative risk analysis should make it possible to quantify the size of losses. However, quantification is challenging as it requires an appropriate input to quantify the risks. There is no single methodology allowing to determine the quantitative value of risk. This is primarily due to the lack of the required amount of statistical information on the possibility of a specific threat. Secondly, determining the cost (and resulting value) of a specific information resource plays an important role and is often a challenging task [11–13]. For example, a business can quantify and indicate the cost of the equipment and media storing a specific information resource but is likely to be unable to determine the exact cost of the data on this equipment and media or the financial consequences of losing it.

Vulnerability and threat are additional key concepts for assessing information security risks. A vulnerability is a defect or weakness in a protected asset that may compromise its confidentiality, integrity, or availability. A threat is a potential opportunity to disrupt information security. An attacker materializes a threat by exploiting a vulnerability in a resource and mounting an attack [1]. Basically, to compile a risk model, the following components are needed to be considered:

1. Assets;
2. An application domain;
3. A list of potential threats to the assets;
4. A list of potential vulnerabilities;
5. A list of countermeasures and recommendations for risk mitigation [14,15].

Vulnerabilities related to information systems vary from configuration flaws that allow access to assets to third parties with limited access information to software errors.

The period between the moment when the vulnerability is identified and can be exploited and the moment it is eliminated represents the window of opportunity associated

with this vulnerability. The increasing complexity of software combined with the fast-paced release of new applications and architectures leads to the continuous emergence of new vulnerabilities and the means to exploit them. The permanent presence of one or more windows of opportunity requires organizations to continuously monitor the spectrum of user interactions and countermeasures taken as quickly as possible.

There are two widely used formulas for quantitative risk assessment supported by a number of prior research studies and standards [1,16–20]. The following descriptions and associated Equations (2)–(7) summarize the respective categories.

The first approach considers the causality between threat and damage [16,17]. It includes four factors: the probability of an event occurring, the amount of damage, the probability of the threat, and the magnitude of vulnerability. The magnitude of risk, as shown in (2), is a product of the probability of event and amount of damage. *Probability of event*, introduced by (3), indicates the likelihood of exploiting the existing vulnerabilities, successfully implementing the threat to the asset, and inflicting damage to the organization and is a product of the *probability of threat*, which determines how likely it is for the threat to materialize, and the *magnitude of vulnerability*, which defines how likely it is for a threat to materialize using a specific vulnerability. The *amount of damage* aims to quantify the extent of the effect on the infrastructure:

$$[Magnitude\ of\ risk] = [Probability\ of\ event] \times [Amount\ of\ damage] \quad (2)$$

where the value of *Probability of event* is determined by the formula:

$$[Probability\ of\ event] = [Probability\ of\ threat] \times [Magnitude\ of\ vulnerability] \quad (3)$$

where *Probability of event* is a probability of successful implementation of the threat to the asset using vulnerabilities and damage to the organization; *Probability of threat* is a probability that the threat to the asset will be realized (the success or failure of the threat is determined by the magnitude of the vulnerability); *Magnitude of vulnerability* is a likelihood that in the event of a threat to an asset, that threat will be successfully exploited using that vulnerability.

The second formula for quantitative risk assessment also includes the *Magnitude of the vulnerability* and the *Amount of damage*, but it focuses instead on the amount of effort required to mount an attack, expressed through the *Number of attempts to implement the threat*:

$$\begin{aligned}[Magnitude\ of\ the\ risk] = [Number\ of\ attempts\ to\ implement\ the\ threat] \times \\ [Magnitude\ of\ the\ vulnerability] \times [Amount\ of\ damage]\end{aligned} \quad (4)$$

For each risk, we calculate the Annual Loss Expectancy (*ALE*), which is a business-friendly measure of a risk in a quantitative risk assessment approach [19,20]. *ALE* requires defining a number of additional parameters: Annual Rate of Occurrence (*ARO*), Single Loss Expectancy (*SLE*), Annual Loss Expectancy, Asset Value, and Exposure Factor, further defined below. The value of *ALE* characterizes the potential annual losses (risk). It is calculated based on *ARO* and the *SLE* for each risk:

$$ALE = ARO \times SLE \quad (5)$$

The *ARO* is a business-friendly measure of the *probability of occurrence* of an event, which helps in terms of the annual budget. *ARO* shows the likelihood of a specific threat to be realized within a specified period (most often, in one year) and can also take values in the range from 1 to 3 (low, medium, high).

SLE is the *monetary value expected* from the occurrence of a risk on an asset. It follows from the asset value and how much of that asset value will be taken away in the event of risk being realized. Another way to calculate ALE is

$$ALE = ARO \times AV \times EF. \quad (6)$$

where *AV* (Asset Value) is a resource cost, reflecting the value of a particular information resource. With a qualitative assessment of risks, the cost of a resource, as a rule, ranges from 1 to 3, where 1 is the minimum cost of the resource, 2 is the average resource cost, and 3 is the maximum resource cost. For example, in the banking information system, an automated service will have the rank $AV = 3$, while a separate information terminal will have an $AV = 1$. The *EF* (Exposure Factor) is the degree of vulnerability of the resource to the threat. This parameter demonstrates how vulnerable a resource is to the threat under consideration. As part of qualitative risk assessment, this value also ranges between 1 and 3, where 1 is the lowest degree of vulnerability (minor impact), 2 is medium (there is a high probability of resource recovery), and 3 is the highest degree of vulnerability (complete replacement of the resource is required after the threat has been disposed of). For example, considering a banking organization, the same server of an automated banking system is characterized by the greatest availability, carrying, therefore, the maximum associated threat of 3.

After making the initial risk assessment, the calculated values need to be ranked according to their importance to determine the low, medium, and high levels of information risks.

In practice, risk assessment is always performed at a certain level of detail. All components of the risk can be broken down into smaller components or can be grouped to obtain more general estimates. It all depends on the goals of the organization: to obtain general information about the state of possible threats and vulnerabilities or to build a quality comprehensive information security system. Therefore, the equation can be used to calculate the risk:

$$[\textit{Magnitude of group of risks}] = [\textit{Number of attempts to implement the group of threats}] \times [\textit{Total magnitude of the vulnerabilities}] \times [\textit{Amount of total damage/losses}] \quad (7)$$

where the *Number of attempts to implement the group of threats* is the expected number of attempts to implement threat groups during the year; and the *Total magnitude of the vulnerabilities* is the total probability that in the event of threats to assets, these threats will be successfully implemented using this group of vulnerabilities. The *Amount of total damage/losses* is the amount of damage in case of loss of all assets to which threats are realized. In general, the magnitude of the risk depends on the asset values, the threats and related probabilities of occurrence of a dangerous event for assets, the ease of implementation of threats exploiting specific vulnerabilities, and the existing or planned remedies that reduce vulnerabilities, threats, and adverse effects.

The stages of risk analysis, in general for most of the methods used, are shown in Table 1.

Depending on the needs of the organization and the conclusions of its management regarding the value of the asset, the risk may be eliminated, reduced, transferred, or approved. Eliminating the risk would be achieved when refusing to use the resource. Reducing the risk would require, for example, the introduction of means and mechanisms of protection that reduce the likelihood of a threat or the coefficient of destructiveness. The risk could also be transferred to an insurance company or a third party responsible for the respective element, who, in the event of a security threat, will bear the costs associated with the loss, instead of the owner of the information system. Finally, the risk can be approved by developing an action plan and setting in place appropriate conditions [21].

Table 1. Stages of risk assessment.

Stage	Input	Risk Assessment Stages	Output
1	Hardware, software, system interfaces, data and information, personnel, system mission	Determining the characteristics of the information system	System boundaries System functions Criticality of the system and data System and data sensitivity
2	Preliminary risk assessment reports Auditors' comments Security requirements Security test results	Identification of vulnerabilities	List of potential vulnerabilities
3	History of attacks on the system Information from response teams, media, law enforcement	Threat identification	List of potential threats
4	Available security regulators Planned security regulators	Analysis of security regulators	List of available and planned security regulators
5	Motivation of the source of threats Threat source resources The nature of the vulnerability Existing countermeasures	Determining the probability of threat realization	Probability rating
6	Analysis of the impact on the mission of the organization Assessment of asset criticality Data criticality Data Vulnerability	Definition of impact Loss: confidentiality, availability, integrity	Impact rating
7	Probability of threat realization Level of influence Adequacy of existing and planned countermeasures	Risk identification	Risks and their levels
8	Risk levels	Countermeasures	List of countermeasures
9	Risk levels	Resulting documentation Risk analysis report	Reports

Risk acceptance varies between organizations. Its level depends on a sum of factors, including the specific business goals of the company, the risk security risk profile, number of customers, financial impact, and portion of investment or budget dedicated to risk management [6]. The risk appetite or risk tolerance sets the boundaries for prioritizing which risks need to be addressed. A company with a high risk appetite may approve of more risk for a higher reward associated with the risk, while a company with a low risk appetite would seek less uncertainty, for which it would accept a lower return. Setting the appetite is critical to managing the business effectively and efficiently to help an organization know where to invest time and resources.

The purpose of any approach to information security risk assessment is to study the risk factors and make the best decision on risk management. Risk factors are the main parameters that are taken into account when assessing risks. There are only seven such parameters: asset, losses, threat, vulnerability, control mechanism, amount of average annual losses, and return on investment.

4. Analysis of Existing Methods of Information Security Risk Assessment

In order to solve the problem of information security risk assessment, many software packages have been created according to the developed methods, which are now used by enterprises and auditors [22]. There are over 30 methodologies and frameworks that can be used for IT security risk assessment [22–26]. A complete analysis of the entire risk analysis spectrum is beyond the scope of this work; in order to provide a substantial coverage based on the current usage trends, we focus on the subset that is most commonly used by enterprises, focusing on methodologies that include a budget decision. As a result, we do not consider frameworks designed for audit, IT governance, and certification, such as ISO/IEC 27001:2005 [1], ISO/IEC 15408:2006 (Common Criteria for Information

Technology Security Evaluation), COBIT (ISACA), and NIST SP-800 [16] standard whose main purposes are audit, IT governance, and certification. This section highlights the most significant ones.

The Central Computer and Telecommunications Agency (CCTA) Risk Analysis and Management Method (CRAMM) is one of the most common alternatives of risk control [27]. Risk analysis using this method involves identifying and calculating risk levels based on estimates assigned to resources, threats, and resource vulnerabilities. Risk control is the identification and selection of countermeasures that can reduce risks to a level that the company can take.

The study of the system using CRAMM is carried out in five stages:

1. Initiation, which produces a description of the boundaries of the information system, its main functions, categories of users, and personnel involved in the survey;
2. Definition and valuation of assets, to describe and analyze everything related to determining the value of system resources. At the end of this stage, it is determined whether the customer is satisfied with their existing practice or whether they need a full risk analysis. In the latter case, a model of information system will be built from the position of the information security;
3. Threat and vulnerability assessment (optional stage, depending on whether the customer satisfies the basic level of information security), aiming to deliver a full risk analysis. Finally, the customer receives identified and assessed levels of threats and vulnerabilities for its system;
4. Risk analysis, to assess the risks either on the basis of assessments of threats and vulnerabilities in full risk analysis or by using simplified techniques for the basic level of security;
5. Identification of countermeasures.

Following the above stages, the process then selects the criteria applicable to this information security and assesses the damage on a scale with values from 1 to 10. In the CRAMM descriptions, as an example, the rating scale is given according to the criterion "Financial losses associated with the restoration of resources" as follows:

- 2 points—less than USD 1000;
- 6 points—from USD 1000 to USD 10,000;
- 8 points—from USD 10,000 to USD 100,000;
- 10 points—over USD 100,000.

All the necessary input for the CRAMM methodology comes in the form of expert assessments and responses to surveys of employees of the organization on aspects of their use of various resources. These surveys are also formulated based on the data on the information system of the organization entered by experts [27]. This process of collecting data can be cumbersome and time-consuming, which represents one of the most significant drawbacks of this approach. From a processing perspective, the CRAMM software then generates a list of unambiguous questions for each resource group and each of the 36 threat types. The level of threats is rated, depending on the responses, as very high, high, medium, low, and very low. The level of vulnerability is assessed, depending on the answers, as high, medium, and low. Thus, CRAMM is an example of a calculation method in which the initial estimates are received at a qualitative level and then translated to a points-based quantitative assessment. One issue of CRAMM is that its implementation cannot be reused, as it cannot remember or reuse previous results as factors that affect risk parameters.

Facilitated Risk Analysis Process (FRAP) is a technique where information security provision is considered as part of the risk management process [28]. Within FRAP, risk management begins with risk assessment: properly documented findings are the basis for decisions to strengthen the security of the system in the future. Once the assessment is complete, a cost–benefit analysis is performed to identify the protection tools needed to reduce the risk to an acceptable level for the organization. Creating a "threat" list, according to the FRAP methodology, can use several approaches:

- Lists of possible threats prepared in advance by experts;
- Analysis of adventure statistics in this information system;
- "Brainstorming" conducted by employees of the company.

When the list of threats is complete, each of them is compared with the probability of occurrence by an expert, followed by an assessment of the damage that may be caused by this threat. The level of threat is estimated based on the obtained values, thus assessing the level of risk for the unprotected IP, which further shows the effect of the introduction of information security tools. The last stage of this technique is documentation. When the risk assessment is completed, its results should be documented in detail in a standardized format for further use or more in-depth analysis. The list of basic stages of risk assessment largely resembles the stages and approach employed by other methods but FRAP provides a slightly more in-depth view of a system and its vulnerabilities. However, the FRAP techniques require expert communication and meetings inside companies which makes the collecting data process time-consuming.

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a methodology developed by the Software Engineering Institute (SEI) at Carnegie Mellon University for the identification and management of information within an organization. According to this method, the whole process of analysis is carried out by the staff of the organization, without the involvement of external consultants, following a self-directed approach. This involves the creation of a mixed group that includes both technicians and managers at various levels, which provides a comprehensive assessment of possible security incidents, together with the business implications of the development of countermeasures [29].

OCTAVE provides three phases of analysis:

- Development of a profile of threats related to the asset;
- Identification of vulnerabilities;
- Development of security strategies and plans.

A profile described by the OCTAVE method follows a tree structure, as shown in Figure 3. Such a threat profile is created for each critical asset, with one tree structure for each category of threat [30]. When creating a threat profile, it is recommended to limit the number of technical details, as this is the task associated with the second stage of the methodology. In OCTAVE, risk assessment is provided primarily through the perspective of the expected damage, without an assessment of probability, using a qualitative high/medium/low scale. The expected damage is represented as a combination of financial damage, damage to the company's reputation, life and health of customers and employees, and damage that can cause legal prosecution as a result of an incident.

OCTAVE has a catalog of countermeasures to mitigate the threat landscape. Unlike other methods, it does not imply the involvement of third-party experts in the study of information security, and all documentation on OCTAVE is publicly available and free of charge, making the methodology especially attractive for enterprises with a tightly limited budget allocated for information security. The main advantage provided by OCTAVE is its modular implementation. Given its exhaustive analysis, organizations may choose to implement portions of the workflow that they find appropriate. OCTAVE has two variants: OCTAVE-S and OCTAVE Allegro. OCTAVE-S has fewer processes, nevertheless adhering to the overall OCTAVE philosophy [31] and thus simplifying application for SMBs. OCTAVE Allegro is a later variant, which focuses on protecting information-based critical assets.

The RiskWatch methodology is another alternative risk assessment method that uses the expected annual losses ALE and returns on investment as criteria for assessing and managing risks. RiskWatch is focused on accurately quantifying the ratio of losses from security threats and the cost of creating a protection system. The RiskWatch product is based on a four-stage risk analysis technique [32].

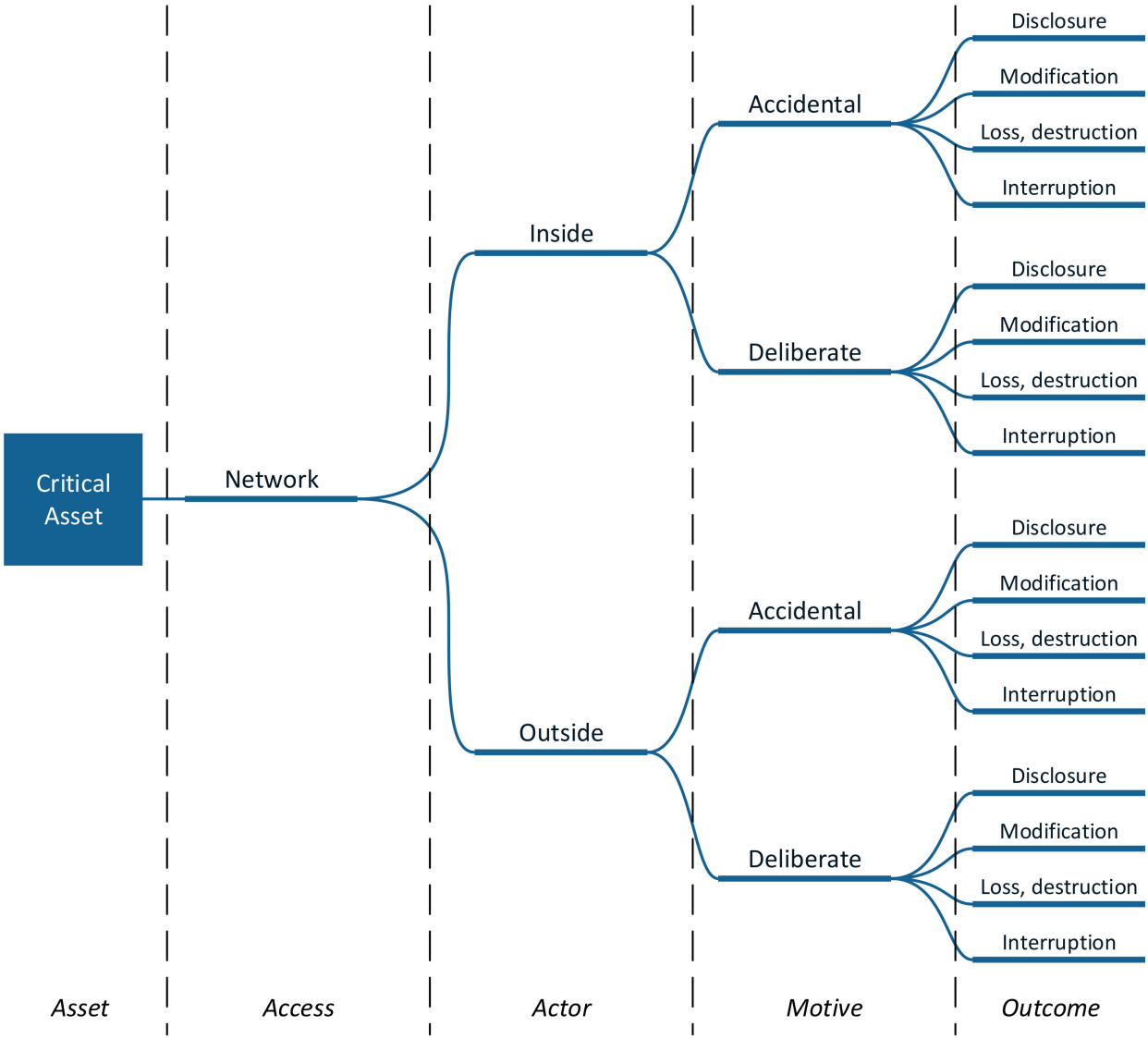

Figure 3. The variant tree is used to describe the profile in the OCTAVE method.

The first stage is to determine the subject of research using the following parameters: type of organization, system composition, and basic security requirements. The second stage is the input of data describing the specific characteristics of the system. Data can be imported from reports created by computer network vulnerability research tools, describing resources, losses, and incident classes. Incident classes are obtained by comparing the category of losses and the category of resources. It also sets the frequency of each of the identified threats, the degree of vulnerability, and the value of resources. The third stage is quantitative risk assessment [11]. This tool allows the assessment of both the risks that currently exist in the enterprise and the benefits that may bring the introduction of physical, technical, software, and other means and mechanisms of protection. The resulting reports and graphs provide sufficient decision-making input material for managing and changing the security system of the enterprise. In the fourth step, reports are generated.

The RiskWatch technique divides the information system into several profiles and uses the specified system for the account of risks of information security of the enterprise. The RiskWatch family includes several software products for various types of security audits: an intelligent physical security risk assessment platform, an information security

risk management platform, a compliance assessment and management platform, a supplier security risk assessment platform, and a vendor security risk assessment platform.

Thus, RiskWatch makes it possible to assess not only the risks that the enterprise currently has but also the benefits that the introduction of physical, technical, software, and other means and mechanisms of protection can bring. The prepared reports and graphs provide material sufficient for making decisions on changing the enterprise security system.

The matrix-based approach of risk analysis links assets, vulnerabilities, threats, and controls and determines the importance of the various controls to the assets of the organization [33], which are perceived to be significant from the point of view of objects that can be both material and intangible. The matrix methodology includes three separate but related matrices: a threat matrix, a vulnerability matrix, and a control matrix to collect the data that are required for risk analysis [34]. The vulnerability matrix contains the relationship between assets and vulnerabilities in the organization, the threat matrix contains the relationship between vulnerabilities and threats, and the control matrix contains the relationships between threats and controls. The value in each cell of the matrix shows the value of the relationship between the row and column element, using the standard qualitative low/medium/high rating system.

It is convenient to use the scale for measuring the impact:

- "0" is no impact;
- "1" is weak;
- "3" is moderate;
- "9" is strong.

One of the main advantages of this method is that it can be applied to almost any organization. The methodology contains convenient matrix templates that can be improved with the advent of new information for analysis. This method can be used independently without contacting specialists.

MEHARI methodology [35] provides a structured approach to risk assessment that is designed to assist in the implementation of ISO 13335, 27001, and 27005 standards to ensure certification. Risk analysis is scenario-based; for each scenario, a database is compiled and documented either using tables that are integrated into Microsoft Excel or OpenOffice or connecting to specialized software such as Risicare, which has a user-friendly interface, as well as modeling, visualization, and optimization capabilities.

MEHARI provides an opportunity to assess the risk factors and threats both qualitatively and quantitatively. For the assessment, a structured risk model is used that takes into account "risk reduction factors". The risk analysis process is implemented in seven stages:

1. Risk identification to identify what is under the risk;
2. Risk analysis to establish seriousness;
3. Risk evaluation to decide whether the risk is acceptable or not;
4. Risk treatment to decide if one needs to accept, redact, transfer, or avoid risk;
5. Developing the action plan;
6. Implementing the action plan;
7. Monitoring and steering direct management of risks.

Although this methodology is simple to implement, free, and compatible with the ISO information security standards, it requires a large "knowledge base" of risks at the initial stage to support semi-automatic risk assessment procedures based on a set of input factors. A number of studies have considered alternatives for improving the process automation, such as [36], which aims to combine MEHARI with risk forecasting.

CORAS was originally developed as part of a European project but has not been funded since 2003. However, this non-profit methodology is supported by the efforts of volunteers and has its own community [37]. It is based on the ISO 27002 standard and is ISO 27005 compliant. CORAS uses a special UML-based diagramming language for visualization and risk assessment. The language offers five types of basic diagrams: asset diagrams, threat diagrams, risk diagrams, treatment diagrams, and treatment overview diagrams.

The method describes eight sequential steps:

1. Preparatory: define the purpose of the assessment and the depth of analysis.
2. Requirements analysis: working with the customer to reach a common understanding of the overall goals and planning, as well as the purpose, focus, and scope of the assessment.
3. Critical appraisal: investigate the company infrastructure and its most valuable assets. Several high-level threat scenarios, vulnerabilities, and risks have been agreed upon for further study. Refined targets and detailed target descriptions are documented using the CORAS language.
4. Identification of risk assessment criteria that will be used in the future. This step also checks whether the customer approves of the detailed description of the goal and its context, including assumptions and preconditions.
5. Brainstorming: workshop-based activity that aims to identify as many risks as possible.
6. Risk level assessment: interdisciplinary brainstorming session that aims to determine the likelihood and consequences of each of the previously identified risks.
7. Making decisions on risks.
8. Evaluate and compare possible treatments and mitigation.

CORAS's core strengths, aside from the fact that it is free, are its use of a model-based approach for risk assessment and its methodology, written in an accessible language for managers and IT experts. Its use of diagrams facilitates communication between different stakeholder groups. The most significant drawback of CORAS is its duration, as the process requires a significant number of meetings with personnel from different backgrounds, and the actual risk assessment is performed only in the second half of the analysis, starting from step 5 (risk identification, risk analysis, risk assessment, and risk treatment).

Table 2 summarizes the defining characteristics of the risk assessment methods discussed within Section 3 in terms of approach used and input/output parameters. For an integrated presentation of the risk parameters [38], we used parameters from Section 3: V—vulnerability, T—threat, I—impact, M—measure of risk (either qualitative or quantitative, QLT and QTY respectively), F—frequency, L—losses, P—probability, E—events that can lead to a violation of information security, and C—controls that needed to be in place to treat the identified risk.

Table 2. Risk assessment methods and characteristics.

Method	Risk Calculation		RA Approach
	Input Factors *	Output Factors	
CORAS [37]	E, V, M, I, D	P, M, C	QLT
CRAMM [27]	E, M, F, P, T, I, V	E, A, M, F, P, L, C	QLT
FRAP [28]	M (QLT) T, C	P, M (QTY)	QLT
MEHARI [35]	E, C	I, M	QLT, QTY
OCTAVE [29]	E, T, V, M	I, M C	QLT
Risk Matrix [33]	D, M, V, T, C	P, I	QLT, QTY
RiskWatch [32]	E, I, F, L, V	M, P, L, C	QTY

* Assets as input are used in every method.

Based on the analysis carried out, information security specialists can then choose the appropriate methods and tools they need, according to the data available at the input or the results they want to get at the output. For example, if the process requires information about the measure and probability of risk at the output, as well as information about possible losses, then one can use the RiskWatch method. If the input includes information about the action as well as the extent and the likelihood of the risk, then one can use the CRAMM method.

5. Shortcomings of Existing Methods and Possible Solutions

Existing risk assessment methodologies mostly differ in the applied risk assessment scales: quantitative or qualitative. The output of the algorithm of quantitative methodology

is the numerical value of risk. The information on unexpected events and threats is usually used as input for evaluation. However, the frequent lack of sufficient statistics leads to a decrease in the adequacy of the results. Qualitative techniques are more common, but they use overly simplistic scales, which usually contain three levels of risk assessment (low, medium, high). The assessment carried out by interviewing experts and by using intelligent methods is still insufficient. Moreover, such results cannot be reused.

In connection with the above shortcomings, experts are actively looking for a technique that would give a high-quality outcome that can adapt to the constant changes of the threat landscape, exclude the inadequate and irrelevant expert assessments, and allow reuse of previous evaluations. The most promising method in this area is the artificial neural network (ANN) approach, which addresses the challenges of existing methods, particularly with regards to flexibility and adaptability, although it requires a lot of time and intellectual resources [39–42]. In addition, the ANN has intelligent features such as self-learn, and thus it is possible to find the best way to solve the problem, accumulating information about external and internal processes.

The neural network module acts as the main mechanism for calculating the magnitude of the risk associated with the vulnerability. First, a fuzzy model of information systems needs to be constructed where the input variables of the system are the values of three risk parameters in the range [0, 1] obtained by interviewing experts when following one of the risk assessment methods described earlier. According to Equations (3), (4) and (7), these three parameters correspondingly represent the approximate probability that the attacker will exploit the vulnerability, the level of damage, and the level of vulnerability (also described as the degree of difficulty when aiming to eliminate the vulnerability). The neural network can use fuzzy logic during calculation, while the quality and accuracy can be ensured by the ability of the neural network to learn and by the process of correlation of synaptic weights. The output is a system that receives the input values of threat, damage, and vulnerability and calculates a quantitative indicator of risk. The user is able to obtain risk values for various vulnerabilities of the automated system and draw appropriate conclusions about the overall level of risk. The same methodology can be applied to all the models presented in Table 2, where the parameters from the risk calculation column can be used as input for the fuzzy model.

This approach to assessment is new and can solve the existing problems due to the shortcomings of the usual, widely used method of risk assessment based solely on expert assessment of the level of threats, losses, and vulnerabilities.

Another approach that can simplify and speed up the process of risk assessment is using ontology-based modeling [43–47]. This approach uses semantic elements defined during risk analysis and provides an easy way of duplicating the data once the object or process has been described. The risk factors can be described and structured using different formalization languages (Web Ontology Language, natural language, UML). The advantage of this modeling approach is that the model can be reused by the company during the next risk evaluation exercise or can be adapted to a new application. This can solve the problem of some of the methods regarding the reuse of survey results.

6. Conclusions

Beyond the concept definition of information risk assessment, the entry provides an insight into the qualitative and quantitative risk assessment methods, highlighting the shortcomings and details of the process. A number of software packages have been created that allow automating individual stages of a specialist's work, but, as highlighted, they provide mainly a series of mathematical calculations or the formation of reports or other documentation and are not able to automate the technical risk analysis and auditing activities or to train the system when re-performing the operation. In almost all risk analysis methodologies, the processes of qualitative and quantitative assessment are separated. Qualitative information on the levels of threats and vulnerabilities is collected first, followed by a quantitative expert assessment of these parameters.

Due to their shortcomings, both qualitative and quantitative methods are considered non-complete, subjective, including an element of randomness, and difficult to update or reuse. Section 5 provides the necessary horizon scanning, focusing on AI-based methods, fuzzy logic, and artificial neural networks (ANNs) and their usage for a more effective calculation of risk, considering the mix of qualitative input parameters such as threat, damage, and vulnerability. The application of an artificial neural network can help in evaluating information risk security since they have self-learn ability, can solve uncertain problems, and are suited for quantity data processing. Other fuzzy logic models such as Bayesian networks, hidden Markov, and decision tree models can also be used with other types of pattern recognition to solve difficult risk assessment problems. These are the technologies that future research must focus on in order to facilitate, simplify, and automate the information risk assessment process, as well as increase the resilience of operations and business processes.

Author Contributions: Conceptualization, I.K. and V.S.; methodology, V.S.; investigation, T.B. and B.G.; writing—original draft preparation, I.K.; writing—review and editing, B.G., V.S. and T.B.; visualization, V.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The author declares no conflict of interest.

Entry Link on the Encyclopedia Platform: https://encyclopedia.pub/13396.

References

1. ISO Standard. *Information Technology—Security Techniques—Information Security Risk Management*; ISO/IEC 27005:2018; ISO Standard: Geneva, Switzerland, 2018.
2. Knight, F.H. *Risk, Uncertainty and Profit*; Hart, Schaffner and Marx, Houghton Mifflin: Boston, MA, USA, 1921.
3. NIS Cooperation Group; European Commission. Cybersecurity Incident Taxonomy. 2018. Available online: https://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf (accessed on 11 January 2021).
4. Launius, S.M.; Evaluation of Comprehensive Taxonomies for Information Technology Threats. SANS Institute. 2018. Available online: https://www.sans.org/reading-room/whitepapers/threatintelligence/evaluation-comprehensive-taxonomies-information-technology-threats-38360 (accessed on 11 January 2021).
5. Model Risk Management: Quantitative and Qualitative Aspects. Management Solutions. 2014. Available online: https://www.managementsolutions.com/sites/default/files/publicaciones/eng/Model-Risk.pdf?q=PDF/ENG/Model-Risk.pdf (accessed on 11 January 2021).
6. Wheeler, E. *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up*, 1st ed.; Syngress: Burlington, MA, USA; Elsevier Inc.: Waltham, MA, USA, 2011.
7. Buriachok, V.; Sokolov, V.; Skladannyi, P. Security Rating Metrics for Distributed Wireless Systems Threats. In Proceedings of the 8th International Conference on "Mathematics, Information Technologies, Education", Lviv, Ukraine, 2–4 June 2019; Volume 2386, pp. 222–233.
8. Williams, J.; OWASP Risk Rating Methodology. OWASP. Available online: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology (accessed on 11 January 2021).
9. Kuzminykh, I.; Yevdokymenko, M.; Ageyev, D. Analysis of Encryption Key Management Systems: Strengths, Weaknesses, Opportunities, Threats. In Proceedings of the IEEE International Scientific-Practical Conference Problems of Infocommunication, Science and Technology (PIC S&T-2020), Kyiv, Ukraine, 6–9 October 2020.
10. Kuzminykh, I.; Ghita, B.; Shiaeles, S. Comparative Analysis of Cryptographic Key Management Systems. In *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*; Galinina, O., Andreev, S., Balandin, S., Koucheryavy, Y., Eds.; Springer: Cham, Switzerland, 2020; Volume 12526, pp. 80–94.
11. Yang, S.; Ishtiaq, M.; Anwar, M. Enterprise risk management practices and firm performance, the mediating role of competitive advantage and the moderating role of financial literacy. *J. Risk Financ. Manag.* **2018**, *11*, 35.
12. Rios, E.; Rego, A.; Iturbe, E.; Higuero, M.; Larrucea, X. Continuous quantitative risk management in smart grids using attack defense trees. *Sensors* **2020**, *20*, 4404. [CrossRef] [PubMed]
13. Generalov, I.G.; Suslov, S.A. Methodological approaches to assessing the competitiveness of organizations. *Vestnik NGIJeI* **2016**, *9*, 31–38.
14. Kuzminykh, I.; Carlsson, A. Analysis of Assets for Threat Risk Model in Avatar-Oriented IoT Architecture. In *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*; Galinina, O., Andreev, S., Balandin, S., Koucheryavy, Y., Eds.; Springer: Cham, Switzerland, 2018; Volume 11118, pp. 52–63.

15. Kuzminykh, I. Avatar Conception for "Thing" Representation in Internet of Things. In Proceedings of the 14th Swedish National Computer Networking Workshop, Karlskrona, Sweden, 31 May–1 June 2018.
16. NIST Special Publication (SP) 800-30, Revision 1. Guide for Conducting Risk Assessments. Available online: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (accessed on 22 July 2021).
17. GB/T 20984-2007. *Information Security Technology: Risk Assessment Norm of Information System*; National Standard of the People's Republic of China; Standardization Administration of PRC: Beijing, China, 2007.
18. Cole, E. (Ed.) Chapter 4—Risk-Based Approach to Security. In *Advanced Persistent Threat*; Syngress: Waltham, MA, USA, 2013; pp. 77–96.
19. Wawrzyniak, D. Information Security Risk Assessment Model for Risk Management. In *Trust and Privacy in Digital Business (TrustBus)*; Fischer-Hübner, S., Furnell, S., Lambrinoudakis, C., Eds.; Springer: Berlin/Heidelberg, Germany, 2006; Volume 4083, pp. 21–30.
20. Lee, M.-C. Information security risk analysis methods and research trends: AHP and fuzzy comprehensive method. *Int. J. Comp. Sci. Inf. Tech.* **2014**, *6*, 29–45.
21. Alexander, D.; Finch, A.; Sutton, D.; Taylor, A. *Information Security Management Principles*; BCS Learning & Development Ltd.: Swindon, UK, 2013.
22. Watson, D.; Jones, A. Chapter 5: Risk management. In *Digital Forensics Processing and Procedures*, 1st ed.; Syngress: Waltham, MA, USA, 2013.
23. Gritzalis, D.; Iseppi, G.; Mylonas, A.; Stavrou, V. Exiting the Risk Assessment Maze: A Meta-Survey. *ACM Comput. Surv.* **2018**, *51*, 1–30. [CrossRef]
24. Ionita, D. Current Established Risk Assessment Methodologies and Tools. Master's Thesis, University Twente, Enschede, The Netherlands, 2013. Available online: https://essay.utwente.nl/63830/1/MSc_D_Ionita.pdf (accessed on 29 June 2021).
25. Lutskiy, M.G.; Ivanchenko, E.V.; Kazmirchuk, S.V.; Okhrimenko, A.A. Modern Information Risk Management. *Inf. Prot.* **2012**, *1*, 1–6. [CrossRef]
26. ENISA. Inventory of Risk Management. Risk Assessment Methods. Available online: https://www.enisa.europa.eu/topics/threat-risk-manage-ment/risk-management/current-risk/risk-management-inventory/rm-ra-methods (accessed on 29 June 2021).
27. CRAMM Version 5.1 User Guide; Insight Consulting: 2005. Available online: https://pdfcoffee.com/cramm-version-51-user-guide-pdf-free.html (accessed on 29 June 2021).
28. Peltier, T.R. Facilitated Risk Analysis Process (FRAP). In *Information Security Risk Analysis*, 1st ed.; Auerbach Publications: New York, NY, USA, 2001.
29. Caralli, R.A.; Stevens, J.F.; Young, L.R.; Wilson, W.R. *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*; CMU/SEI-2007-TR-012 Technical Report; Software Engineering Institute, Carnegie Mellon University: Pittsburgh, PA, USA, 2007.
30. Alberts, C.; Dorofee, A. OCTAVE Threat Profiles. Software Engineering Institute, Carnegie Mellon University. Available online: http://130.18.86.27/faculty/warkentin/SecurityPapers/Merrill/AlbertsDorofee_OCTAVEThreatProfiles.pdf (accessed on 11 January 2021).
31. Wangen, G.; Hallstensen, C.; Snekkenes, E. A framework for estimating information security risk assessment method completeness. *Int. J. Inf. Secur.* **2018**, *17*, 681–699. [CrossRef]
32. Manage Risk Meet Compliance Improve Security. Available online: https://riskwatch.com/#productoverview (accessed on 11 January 2021).
33. Goel, S.; Chen, V. Information Security Risk Analysis—A Matrix-Based Approach. Available online: https://www.albany.edu/~goel/publications/goelchen2005.pdf (accessed on 11 January 2021).
34. Kure, H.I.; Islam, S.; Razzaque, M.A. An integrated cyber security risk management approach for a cyber-physical system. *Appl. Sci.* **2018**, *8*, 898. [CrossRef]
35. Mehari. Risk Analysis and Treatment Guide. CLUSIF. 2010. Available online: http://meharipedia.x10host.com/wp/wp-content/uploads/2016/12/MEHARI-2010-Risk-Analysis-and-Treatment-Guide.pdf (accessed on 29 June 2021).
36. Yermalovich, P.; Mejri, M. Risk Forecasting Automation on the Basis of MEHARI. In *International Information Security Conference*; Venter, H., Loock, M., Coetzee, M., Eloff, M., Eloff, J., Botha, R., Eds.; Springer: Cham, Switzerland, 2020; Volume 1339, pp. 34–49.
37. Lund, M.S.; Solhaug, B.; Stolen, K. *Model-Driven Risk Analysis*; Springer: Berlin/Heidelberg, Germany, 2011.
38. Korchenko, A.G.; Ivanchenko, E.V.; Kazmirchuk, S.V. Integrated Presentation of Risk Parameters. *Inf. Prot.* **2011**, *1*, 96–101. [CrossRef]
39. Zhao, D.-M.; Liu, J.-X.; Zhang, Z.-H. Method of risk evaluation of information security based on neural networks. In Proceedings of the 2009 International Conference on Machine Learning and Cybernetics, Baoding, China, 12–15 July 2009; pp. 1127–1132. [CrossRef]
40. Shang, K.; Hossen, Z. *Applying Fuzzy Logic to Risk Assessment and Decision-Making*; Project Report; Casualty Actuarial Society, Canadian Institute of Actuaries, Society of Actuaries: Ottawa, ON, Canada, 2013; 59p.
41. Paltrinieri, N.; Comfort, L.; Reniers, G. Learning about risk: Machine learning for risk assessment. *Saf. Sci.* **2019**, *118*, 475–486. [CrossRef]

42. Changwei, Y.; Zonghao, L.; Xueyan, G.; Wenying, Y.; Jing, J.; Liang, Z. Application of BP Neural Network Model in Risk Evaluation of Railway Construction. *Complexity* **2019**, *2019*, 2946158. [CrossRef]
43. Nota, G.; Aiello, R.; Di Gregorio, M.P. Ontology Based Risk Management. In *Decision Theory and Choices: A Complexity Approach*; Faggini, M., Vinci, C.P., Eds.; Springer: Milano, Italy, 2010. [CrossRef]
44. Palmer, C.; Urwin, E.N.; Niknejad, A.; Petrovic, D.; Popplewell, K.; Young, R.I. An ontology supported risk assessment approach for the intelligent configuration of supply networks. *J. Intell. Manuf.* **2018**, *29*, 1005–1030. [CrossRef]
45. TajDini, M.; Sokolov, V.; Kuzminykh, I.; Shiaeles, S.; Ghita, B. Wireless Sensors for Brain Activity—A Survey. *Electronics* **2020**, *9*, 2092. [CrossRef]
46. Pileggi, S.F.; Indorf, M.; Nagi, A.; Kersten, W. CoRiMaS—An Ontological Approach to Cooperative Risk Management in Seaports. *Sustainability* **2020**, *12*, 4767. [CrossRef]
47. Mozzaquatro, B.A.; Agostinho, C.; Goncalves, D.; Martins, J.; Jardim-Goncalves, R. An Ontology-Based Cybersecurity Framework for the Internet of Things. *Sensors* **2018**, *18*, 3053. [CrossRef] [PubMed]